UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/671,671	09/28/2000	Young Hun Choi	P56173	7267

8439 7590 01/15/2004

ROBERT E. BUSHNELL
1522 K STREET NW
SUITE 300
WASHINGTON, DC 20005-1202

EXAMINER	
HESSELTINE, RYAN J	
ART UNIT	PAPER NUMBER
2623	6

DATE MAILED: 01/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/671,671	**Applicant(s)** CHOI ET AL.	
	Examiner Ryan J Hesseltine	**Art Unit** 2623	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 October 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 September 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

DETAILED ACTION

Response to Arguments

1. Applicant's arguments on page 11, first paragraph, filed October 14, 2003, with respect to claim 18 have been fully considered and are persuasive. The objection to claim 18 has been withdrawn.

2. Applicant's arguments on page 12 with respect to claim 1, filed October 14, 2003, have been fully considered but they are not persuasive. On page 12, first paragraph, applicant states, "Fitzpatrick's fingerprint recognizing module 82 is disposed beneath the screen 44 of the monitor 40." It is unclear where in the Fitzpatrick patent this statement can be found. Touch screen technology is well known in the art and typically involves a transparent touch-sensitive surface disposed *over* a display element as disclosed in Harkin (USPN 6,327,376, previously cited). Therefore, it is the examiner's view that the multi-point, touch-sensitive surface 70 of Fitzpatrick effectively functions as a "front cover adjacent said screen" as originally stated in claim 1 (now amended). The same argument holds for the remaining independent claims 10-12. The new grounds of rejection are based solely on applicant's amendments to the claims.

3. Applicant's arguments with respect to claims 1 and 10-12 have been considered but are moot in view of the new ground(s) of rejection.

4. Applicant's arguments on page 17 with respect to claims 6-8 have been fully considered but they are not persuasive. On page 17, fifth paragraph, applicant states, "there is no teaching that the encoded signal output from encode/compress circuitry 207 is stored in memory device 223." The examiner agrees with this assertion since it appears that O'Connor does this only to improve data transmission rates between the mouse peripheral device and the computer main

body, but would like to point out that the encode/compress and decode/decompress functions could easily be applied to the storage and retrieval of the fingerprint data to reduce the storage capacity and improve the security of the stored data.

5. Applicant's arguments on page 19 with respect to claim 14 have been fully considered but they are not persuasive. On page 19, third paragraph, applicant states, "contrary to the Examiner's Official Notice, O'Connor teaches it is not necessary to have an established fingerprint database to allow access to the system." The examiner agrees with this assertion, but would like to point out that O'Connor also does not disclose that "pre-approved signatures" (fingerprints) must be registered in advance in order for a user to be authenticated. Obviously it is disclosed that if there are no registered fingerprints (100% valid), the user is given access to the system without identification. This is an obvious security risk, so it would have been obvious to require registration if there are no registered fingerprints to protect possibly sensitive information contained in the computer.

6. Applicant's arguments on page 20 with respect to claim 18 have been fully considered but they are not persuasive. On page 20, last paragraph, applicant states, "The Examiner mistakenly indicates that O'Connor discloses decoding and encoding of fingerprint files..." The examiner agrees that this section was mistakenly referred to since it has been discussed that O'Connor does not truly decode and encode fingerprint "files," but the fingerprint signals are encoded/decoded. The main feature of the claim, determining whether a file stored in said computer system is enabled to be encoded or decoded during file encoding/decoding routine, is not explicitly disclosed by either Fitzpatrick or O'Connor, but Fitzpatrick does disclose

determining access to individual files, and O'Connor was relied upon merely to show that encoding/decoding of data is well known.

7. Applicant's arguments on page 21 with respect to claim 19 have been fully considered but they are not persuasive. On page 21, third paragraph, applicant states, "The Examiner refers us to O'Connor's col. 4, lines 21-26 ... Clearly this section of O'Connor fails to teach the claimed feature." The examiner respectfully disagrees and would like to direct applicant to paragraph 25 of the last Office Action, which refers to various section of the *Fitzpatrick* reference, not the O'Connor reference. The section in question, column 4, line 21-26, of Fitzpatrick, discloses that "manipulation access" is granted to the operator (manager) upon the fingerprint template meeting a specified confidence level. The appropriate program/data is then obtained from memory, which allows the operator to proceed. While this section does not explicitly disclose a fingerprint managing and registering program, such a program is well known in the art and must be present in such a system in order for fingerprint templates to be registered and managed. The examiner believes that this section satisfies the limitation in question.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1, 3-5, 9, 10, 12, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fitzpatrick et al. (USPN 5,420,936, cited on applicant's IDS), hereafter Fitzpatrick, in view of Davis (USPN 6,181,803, newly cited).

10. Regarding claim 1, Fitzpatrick discloses a fingerprint recognizing display system comprising: a monitor (50) having a screen and multi-point, touch-sensitive surface (70) adjacent said screen (column 4, line 3-10); a fingerprint recognizing module (82) included with said monitor, said fingerprint recognizing module including a fingerprint image recognizing unit disposed on a surface of said touch-sensitive surface (column 4, line 14-21), wherein a user desiring access to said fingerprint recognizing display system touches said fingerprint image recognizing unit (column 3, line 52-57); and a computer main body including a fingerprint data base (templates stored in access table) and a fingerprint verifying unit (access granter 76), wherein said fingerprint verifying unit compares fingerprint data transmitted from said fingerprint recognizing module to registered fingerprint data stored in said fingerprint data base and permits said user access to programs stored in said fingerprint recognizing display system when it is determined that the fingerprint of said user matches fingerprint data stored in said fingerprint data base (column 4, line 18-26).

11. Fitzpatrick does not disclose that said fingerprint recognizing module including a fingerprint recognizing unit is disposed on a surface of said front cover surrounding the screen of the monitor. Davis discloses an apparatus and method for securely processing biometric information to control access to a computer node including a biometric device 120 (which reads biometric characteristics including iris patterns, retina patterns, fingerprints, facial geometries, etc.; column 4, line 45-51) which is illustrated as separate from display monitor 111, but it is disclosed that the biometric device may be implemented internally within the casing of the display monitor, casing of the PC, on the input device, etc. (Figure 1; column 3, line 46-58). While neither Fitzpatrick nor Davis explicitly disclose that the fingerprint recognizing unit is

disposed on a surface of the front cover surrounding the monitor screen (Davis shows a CCD camera on top of the monitor in Figure 1), the examiner would like to point out that the fingerprint unit could be placed anywhere on the monitor, but the front cover would be most convenient for the user to reach from a seated position. The examiner would also like to point out that applicant has not provided any particular advantage for the placement of the fingerprint recognition unit. It would have been obvious to one of ordinary skill in the art at the time the invention was made to internally implement a biometric device (fingerprint unit) within the casing of a display monitor as taught by Davis in order to localize the processing of the biometric data clip to provide full identification or authorization functions without requiring an additional task being executed by a host processor of the system (column 2, line 40-47).

12. Regarding claim 10, Fitzpatrick discloses a display apparatus (monitor 50) comprising: a front cover (inherent); and fingerprint recognizing means (multi-point, touch-sensitive surface 70) located on the front side of the screen (column 4, line 3-21). Fitzpatrick does not disclose that said fingerprint recognizing means is located on a front or side panel of said front cover surrounding the display screen. Davis discloses that a biometric device 120 (which reads biometric characteristics including iris patterns, retina patterns, fingerprints, facial geometries, etc.; column 4, line 45-51), which is illustrated as separate from display monitor 111, but it is disclosed that the biometric device may be implemented internally within the casing of the display monitor, casing of the PC, on the input device, etc. (Figure 1; column 3, line 46-58; see above discussion of claim 1).

13. Regarding claim 12, Fitzpatrick discloses a method of recognizing a fingerprint to enable a user to operate a computer system, said method being embodied in an operating system kernel

mode and comprising the steps of: detecting a fingerprint of the user when said user touches a portion of a front cover of a monitor of said computer system (column 4, line 3-21); transmitting (touch driver 74 communicates with fingerprint analyzer 82) fingerprint data corresponding to said fingerprint of said user, when detected, from said monitor to a computer main body of said computer system (column 4, line 14-18); comparing the fingerprint data transmitted from said monitor to registered fingerprint data output from a fingerprint data base included in said computer main body (column 4, line 18-21); and enabling said computer system to be operated by said user when said comparing step indicates that there is a match between the fingerprint data transmitted from said monitor and the registered fingerprint data output from said fingerprint data base (column 4, line 21-26), or disabling (return error message 118) said computer system to prevent operation by said user when said comparing step indicates that there is not a match (access table does not contain a recognized user and selected object match 122) between the fingerprint data transmitted from said monitor and the registered fingerprint data output from said fingerprint data base (figure 5; column 4, line 45-59).

14. Fitzpatrick does not disclose detecting a fingerprint of the user when said user touches a portion of a front cover surrounding the display screen of a monitor. Davis discloses an apparatus and method for securely processing biometric information to control access to a computer node including a biometric device 120 (which reads biometric characteristics including iris patterns, retina patterns, fingerprints, facial geometries, etc.; column 4, line 45-51) which is illustrated as separate from display monitor 111, but it is disclosed that the biometric device may be implemented internally within the casing of the display monitor, casing of the PC, on the input device, etc. (Figure 1; column 3, line 46-58; see above discussion of claim 1).

15. Regarding claim 3, Fitzpatrick discloses that said fingerprint recognizing module also includes: a converter (72) converting analog fingerprint data input from the fingerprint image recognizing unit to digital fingerprint data, and a first communication unit (touch driver 74) transmitting the digital fingerprint data to a second communication unit (fingerprint analyzer 82) in the computer main body (figure 4; column 4, line 7-18).

16. Regarding claim 4, Fitzpatrick discloses that said monitor includes a touch driver 74 (inherently including a microprocessor) communicating with a graphical user interface 78 (inherently including a video card) in said computer main body (figure 4; column 4, line 10-14).

17. Regarding claim 5, Fitzpatrick discloses that said fingerprint recognizing module also includes: a converter (72) converting analog fingerprint data input from the fingerprint image recognizing unit to digital fingerprint data, and said microprocessor (touch driver 74) transmits the digital fingerprint data to a communication unit (graphical user interface 78, fingerprint analyzer 82) in the computer main body (figure 4; column 4, line 7-18).

18. Regarding claim 9, Fitzpatrick does not explicitly disclose that said monitor comprises a cathode ray tube display apparatus or a liquid crystal display apparatus. The examiner takes Official Notice that the use of a cathode ray tube (CRT) and liquid crystal display (LCD) apparatus as monitors for computer systems is well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply the fingerprint recognizing touch screen as taught by Fitzpatrick to CRT- and LCD-type monitors for computer systems.

19. Regarding claim 17, Fitzpatrick discloses that said comparing step includes steps of: checking said fingerprint data transmitted from said monitor and detecting distinctive features thereof (decision block 116); determining whether the detected distinctive features are of good

quality (meets recognition threshold); and outputting an error message (118) when it is determined that the detected distinctive features are not of good quality and returning to said step of detecting a fingerprint of the user (block 102), or performing said comparing step (decision block 122) when it is determined that the detected distinctive features are of good quality (figure 5; column 4, line 45-57).

20. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fitzpatrick in view of Davis and further in view of Srey et al. (USPN 6,141,436, newly cited), hereafter Srey.

21. Regarding claim 11, Fitzpatrick discloses a display apparatus (monitor 50) comprising: a front cover surrounding a display screen (see above discussion of claim 1 with respect to Davis); and fingerprint recognizing means (multi-point, touch-sensitive surface 70) to read a fingerprint image of a user (column 4, line 3-21). Fitzpatrick does not disclose that said fingerprint recognizing means is formed integrally with a power switch placed on a predetermined portion of said front cover. Davis discloses that access control circuitry operating with the biometric processor to authenticate or identify a requesting user may be performed continuously on a periodic basis, or triggered by some action of the requesting user such as depressing a key or flipping a switch (column 5, line 65-column 6, line 9), but Davis also does not disclose that said fingerprint recognizing means is formed integrally with a power switch placed on a predetermined portion of said front cover. The examiner takes Official Notice that placing a power switch on a predetermined portion of a front cover of a display screen is well known in the art. Srey discloses a portable communication device (cellular telephone) having a fingerprint identification system wherein a fingerprint scanner 115 is integrally formed with the power

switch 201 which generates a power on/off signal when actuated by the user's finger (column 5, line 55-column 6, line 2). It would have been obvious to one of ordinary skill in the art at the time the invention was made to integrally form a fingerprint recognizing means with a power switch as taught by Srey in order to allow the finger to generate the actuation force for the power switch when the fingerprint is positioned on the scanner so the processor can determine whether the fingerprint image matches a reference fingerprint, then placing the circuitry in one of two modes responsive to the power on/off signal depending on whether or not the fingerprints match (column 6, line 2-17), and placing the power switch on the front cover of the display screen to allow easy access for a seated user.

22. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fitzpatrick in view of Davis, as applied to claim 1 above, and further in view of Srey.

23. Regarding claim 2, neither Fitzpatrick nor Davis disclose that said fingerprint image recognizing unit is integrally formed with a power switch disposed on the surface of said front cover. The examiner takes Official Notice that placing a power switch on a predetermined portion of a front cover of a display screen is well known in the art. Srey discloses that a fingerprint scanner 115 is integrally formed with a power switch 201, which generates a power on/off signal when actuated by the user's finger (column 5, line 55-column 6, line 2; see above discussion of claim 11).

24. Claims 6-8, 13-16, 18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fitzpatrick in view of Davis as applied to claims 1, 3, and 5 above, and further in view of O'Connor et al. (USPN 5,838,306, cited on applicant's IDS), hereafter O'Connor.

25. Regarding claims 6-8, Fitzpatrick discloses that distinctive feature contact points of captured fingerprints are compared with stored templates, but does not disclose that said fingerprint verifying unit includes: a registered fingerprint decoding unit or a captured fingerprint encoding unit. O'Connor discloses a mouse with security feature including a decoding unit (211) for decoding fingerprint data; an encoding unit (207) for encoding fingerprint data (column 4, line 26-42) including a database (memory device 223) for storing registered (approved) fingerprint data (column 4, line 43-51); a fingerprint matching/recording unit (analysis circuit 213, compare circuit 221) for receiving decoded fingerprint data from said decoding unit, said fingerprint matching/recording unit comparing decoded fingerprint data received from said decoding unit to said registered (approved) fingerprint data and also for outputting said approved fingerprint data to be stored as the registered fingerprint data in said fingerprint database; and a recognizing unit outputting a "pass" signal or a "fail" signal in response to a comparison result output from said fingerprint matching/recording unit (column 4, line 36-51). O'Connor apparently includes the encode/compress and decode/decompress functions only for data transmission purposes between the peripheral device (fingerprint recognizing mouse) and the main body of the computer, but it is an obvious variant to utilize these functions for storage and retrieval of the fingerprint data in order to improve efficiency and security. Additionally, when the captured fingerprint data is encoded/compressed and transmitted from the mouse peripheral unit 101 to a main housing 403, there is inherently present a temporary storage before the fingerprint data is decoded/decompressed for analysis and comparison. It would have been obvious to one of ordinary skill in the art at the time the invention was made to encode/compress approved fingerprint signals and therefore decode/decompress said signals for comparison with

captured fingerprint signals to judge pass or fail of said captured fingerprint signals as taught by O'Connor in order to reduce memory usage and transmission time through compression as well as increase security by encoding the transmitted/stored data (column 4, line 26-32).

26. Regarding claim 13, Fitzpatrick does not disclose determining whether said monitor is a fingerprint recognizing monitor. O'Connor discloses an application security check routine 901 which calls a check fingerprint mouse driver 903 to determine whether said mouse is a fingerprint recognizing mouse. If it is determined that said mouse is not a fingerprint recognizing mouse, said mouse is operating in an abnormal status (wrong mouse) and preventing said computer system from being operated, otherwise said step of detecting a fingerprint is performed (column 6, line 16-21). It would have been obvious to one of ordinary skill in the art at the time the invention was made to determine whether said monitor is a fingerprint recognizing monitor in the same manner as determining whether a mouse is a fingerprint recognizing monitor as taught by O'Connor in order to prevent an unauthorized user from attempting to access the system by using a non-fingerprint recognizing monitor (column 6, line 16-21).

27. Regarding claim 14, O'Connor discloses determining whether said fingerprint data base has been established (contains pre-approved signatures) in said computer main body (Figure 5, step 503) prior to determining whether said monitor (mouse) is a fingerprint recognizing monitor (mouse); and determining whether said monitor (mouse) is a fingerprint recognizing monitor (mouse) when it is determined that said fingerprint data base has been established (Figure 5, step 509; column 5, line 18-30), but O'Connor does not explicitly disclose performing a fingerprint registration routine when it is determined that said fingerprint data base has not been established.

O'Connor also does not disclose a step of storing these "pre-approved" signatures, but it is inherent that this must take place in order of the system to be able to validate a user's identity. O'Connor discloses that if no fingerprint database has been established, the user is given access to the system without identification, which is an obvious security risk if the system contains sensitive information. It would have been obvious to one of ordinary skill in the art at the time the invention was made to perform a fingerprint registration routine when it is determined that said fingerprint database has not been established in order to initialize the fingerprint recognizing system for operation with at least one authorized fingerprint in the database so as to prevent unauthorized users from accessing sensitive information (column 1, line 13-19).

28. Regarding claims 15 and 16, neither Fitzpatrick nor O'Connor explicitly disclose determining whether a keyboard or a mouse of said computer system is operated by said user during operation of a screen protection routine of said computer system; and continuing to run a screen saver program when it is determined that neither said keyboard nor said mouse have been operated, and ending said screen protection routine when said comparing step indicates that there is a match between the fingerprint data transmitted from said monitor and the registered fingerprint data output from said fingerprint data base, and then performing said step of enabling said computer system to be operated by said user. The examiner takes Official Notice that this method of screen protection with the use of a username/password protected screen saver is well known in the art. It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize such a screen protection routine as applied to Fitzpatrick in view of O'Connor using fingerprints in place of a username/password in order to prevent an

unauthorized user from seeing any protected information that may be displayed on the monitor while an authorized user is away.

29. Regarding claim 18, Fitzpatrick does not disclose determining whether a file stored in said computer system is enabled to be encoded or decoded, but does disclose determining whether or not a person has authorized access to certain files (column 3, line 52-65); outputting a message indicating said file can not be accessed when it is determined said person is not authorized (column 4, line 54-59). O'Connor discloses encoding/compressing and decoding/decompressing of fingerprint data (column 4, line 26-32); performing said step of determining whether said monitor (mouse) is a fingerprint recognizing monitor (column 6, line 16-25); and permitting said user to access the computer system when said comparing step indicates that there is a match between the fingerprint data transmitted from said mouse and the registered fingerprint data output from said fingerprint data base (column 4, line 43-57). It would have been obvious to one of ordinary skill in the art at the time the invention was made to determine whether a file stored in said computer system is enabled to be encoded or decoded (or authorized access) as taught by Fitzpatrick, and determining whether said monitor is a fingerprint recognizing monitor as taught by O'Connor in order to increasing security and storage efficiency through encoding/compression (column 4, line 26-36) and prevent an unauthorized user from attempting to access the system by using a non-fingerprint recognizing monitor (column 6, line 16-21).

30. Regarding claim 19, Fitzpatrick discloses that said fingerprint registration routine comprises the steps of: detecting a fingerprint of a manager (operator) when said manager (operator) touches the portion of the front cover of said monitor of said computer system

(column 3, line 52-65); transmitting fingerprint data corresponding to said fingerprint of said manager, when detected, from said monitor to said computer main body of said computer system (column 4, line 3-14); comparing the fingerprint data transmitted from said monitor to registered fingerprint data output from a fingerprint data base included in said computer main body (column 4, line 14-21); and permitting said manager to operate a fingerprint managing and registering program when said comparing step indicates that there is a match between the fingerprint data transmitted from said monitor and the registered fingerprint data output from said fingerprint data base (column 4, line 21-26), or disabling said computer system to prevent operation by said manager when said comparing step indicates that there is not a match between the fingerprint data transmitted from said monitor and the registered fingerprint data output from said fingerprint data base (column 4, line 54-59). While Fitzpatrick does not explicitly disclose a fingerprint managing and registering program, such a program is well known in the art and must be present in such a system in order for fingerprint templates to be registered and managed.

Conclusion

31. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. WO 00/63769 to Han discloses a fingerprint recognition security computer monitor. USPN 5,680,205 to Borza discloses a fingerprint imaging apparatus with auxiliary lens. USPN 6,400,836 to Senior discloses a combined fingerprint acquisition and control device. USPN 6,522,773 to Houdeau discloses a fingertip sensor with integrated key switch. USPN 6,628,757 to Cannon et al. discloses a fingerprint-ID-activated message playback apparatus and method.

32. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ryan J Hesseltine whose telephone number is 703-306-4069. The examiner can normally be reached on Monday - Friday, 8:30 AM - 5 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Amelia Au can be reached on 703-308-6604. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-306-0377.

rjh
January 9, 2004

JINGGE WU
PRIMARY EXAMINER